FILED
OCT 04 2023
Clerk, U. S. District Court
Eastern District of Tennessee
At Knoxville

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

IN THE MATTER OF THE SEARCH OF THE RESIDENCE LOCATED AT 118 MASON AVE. ROCKY TOP TN 37769 AND A BLACK CHEVROLET SUV BEARING TN TAG BPS-5815 REGISTERED TO MICHAEL POTTER LOCATED AT 118 MASON AVE., ROCKY TOP, TN 37769	)	**Docket No. 3:23-MJ-2172** **UNDER SEAL**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

Your affiant, Thomas Evans, an Investigator with the Knoxville Police Department (KPD) Internet Crimes Against Children (ICAC) Task Force and being a Homeland Security Investigations (HSI) Task Force Officer being duly sworn, deposes and states the following:

1. Your affiant has been employed with the KPD since January 22, 1996. Your affiant has been assigned to the Knoxville Police Department's Internet Crimes Against Children Task Force (KPD-ICAC) as a computer examiner and undercover online investigator for the past twenty-three years. KPD-ICAC is responsible for investigating and enforcing federal criminal statutes involving the sexual exploitation of children under Chapter 110 of Title 18, United States Code. As a KPD-ICAC Investigator and Homeland Security Task Force officer, your affiant is authorized to investigate CyberTips submitted to the KPD-ICAC for Missing and Exploited Children. Your affiant has acquired experience in these matters through specialized training and everyday work related to these types of investigations.

2. Your affiant has completed the following training:

- 1996 Knoxville Police Department Training Academy Recruit Class A;
- 1997 Childhelp USA's Professional Training Conference;
- 1997 Identi-Kit 2000 Composite Software Training;

- 1999 Protecting Children On-line provided by Fox Valley Technical College Criminal Justice Department, Appleton, Wisconsin;
- 2000 Advanced Protecting Children On-line provided by Fox Valley Technical College, Criminal Justice Department;
- 2000 National Consortium of Justice Information and Statistics Training directed toward on-line investigation, tracking offenders and data recovery;
- 2000 40-hour course in the National White Collar Crime Data Recovery and Analysis;
- 2000 40-hour Internship with the Dallas Police Department's Internet Crimes Against Children Task Force;
- 40-hour internship with the Maryland State Police in October 2000 focusing on forensic software use in recovering computer-based evidence;
- 2001 Basic Class on EnCase computer forensic software;
- 2001 National Internet Crimes Against Children Training Conference in New Orleans focusing on the use of computer forensic utilities in evidence collection and Online Investigative Techniques;
- 2002 Crimes Against Children Conference in Dallas, TX focusing on online investigative techniques and computer forensic data recovery;
- 40-hour EnCase Intermediate Analysis and Reporting training in Sterling, VA April 2003;
- 2004 Silicon Valley ICAC Task Force Conference in San Jose, CA with focus on online investigations and best computer forensic practice;
- 2004 Crimes Against Children Conference in Dallas, TX with emphasis on online investigative techniques and data recovery;
- December 2004 ICAC Investigative Techniques course in Knoxville, TN focusing on updated investigative techniques in online undercover operations;
- March 2005 EnCase Intermediate Analysis and Reporting course for computer examiners in Sterling, VA;

- May 2005 International Association of Computer Investigative Specialist 80-hour Forensic Computer Examiner Training Program in Orlando, FL;

- Recognized in April 2005 by the International Association of Computer Investigative Specialists as a Certified Electronic Evidence Collection Specialist;

- 2005 National ICAC Conference in Dallas, TX focusing on characteristics of the Internet offender and online undercover operations;

- Knoxville Police Department Basic Investigator Class January 30-February 3, 2006;

- 2006 National Crimes Against Children Conference in Dallas, TX focusing on online undercover Investigative Techniques;

- December 2006 FTK Boot camp held at Pellissippi State Technical College for computer forensic training using the Access Data Ultimate Toolkit software package;

- January 2007 Internet Crimes Against Children Task Force Operation Peer Precision Training in Tallahassee FL focusing on online undercover Peer-to-Peer investigations;

- June 12, 2008, F.B.I. CART ImageScan training concentrating on the use of the ImageScan System for secure computer previews and data recovery;

- April 11- May 14th, 2010, United States Secret Service BCERT Computer Forensic training Hoover, AL;

- February 21-23rd 2012 Tennessee ICAC Training conference in Nashville, TN focusing on cell phone investigations, human trafficking, undercover P2P investigations (instructed), and open-source computer forensic tools;

- USDOJ 2012 National Law Enforcement Training Conference in Atlanta GA April 17-19th, 2012 focusing on P2P undercover investigations, Craigslist undercover investigations, Gigatribe investigations, and the psychological profile of a child pornography collector;

- June 13-17th Internship with the Citrus County Sheriff's Department regarding E Commerce undercover investigations (Operation Summer Nights);

- February 5th - 8th 2013 ICAC eMule P2P investigations;

- March 26-28th 2013– Tennessee ICAC state conference in Nashville, TN focusing on Commercial Sexual Exploitation of Children (CSEC);

- October 28-31, 2013, Tennessee ICAC state conference in Nashville, Tennessee, focusing on forensic preview tools, ICAC legal updates and virtual machine utilization for computer forensics and undercover investigations;

- February 24-26, 2014 – Tennessee ICAC state conference in Nashville, TN, focusing on computer previews, Google Security, and locating wireless devices;

- April 15-17, 2014 – 2014 Regional ICAC Law Enforcement Training on Child Exploitation focusing on court testimony, Ares Peer-to-Peer investigations, National Center for Missing and Exploited Children Law Enforcement Portal, and characteristics of the offender;

- September 18-19, 2014 – Westminster, Colorado ICAC BitTorrent Investigations;

- April 20-22, 2015 – Brentwood, Tennessee – Tennessee ICAC state conference focusing on online undercover chat investigations, legal updates, and human sex trafficking;

- November 11-13, 2015 – Gatlinburg, Tennessee – Tennessee ICAC conference focusing on current chat trends, P2P file sharing investigations, and on scene preview techniques and software;

- March 28-30, 2016 – Nashville, Tennessee – Tennessee ICAC conference focusing on legal updates, use of polygraph in conjunction with child pornography cases and online undercover operations;

- April 18, 2016 – Atlanta, Georgia – National ICAC Conference focusing on online undercover investigations, interviewing offenders, legal updates, psychology of the Internet offender, and on scene computer forensic tools;

- May 2, 2016 – Knoxville, Tennessee – Federal Bureau of Investigation Legal Update Training;

- October 17-19, 2016 – Chattanooga, Tennessee – Tennessee ICAC State Conference focusing on Legal Updates, Anonymity/Darknet, and IP Version 6;

- February 27- March 2017 – Atlanta, Georgia – Freenet Training. Training focusing on anonymous Darknet applications for the trafficking of child pornography; and,

- June 6-8, 2017, Atlanta, Georgia – 2017 National Law Enforcement Training on Child Exploitation. Training focused on the use of tactical polygraph as an investigative tool for identifying child victims, Darknet investigations, and undercover chat strategies to deal with high level offenders.

3. Your affiant has probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a) and 2252A(a), distribution and receipt of child pornography, are located on a device within the residence of 118 Mason Ave, Rocky Top, TN 37769.

4. Your affiant is being assisted in this case by Detective Luethge of the Anderson County Sherrif's Office. Detective Luethge has been a law enforcement officer for eighteen years. Detective Luethge has served two years with Lafollette Police Department, fourteen years with the Oak Ridge Police Department and two years with the Anderson County Sheriff's Office. Detective Luethge is currently assigned to the Tennessee Internet Crimes Against Children Task Force.

5. The information contained within the affidavit is based upon information I have gained from my investigation, my personal observations, my training and experience, and/or information related to me by other law enforcement officers and/or agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning the investigation. I have set forth only the facts which I believe are necessary to establish probable cause to believe that evidence, fruits, and

instrumentalities of the violation of 18 U.S.C. §§ 2252(a) and 2252A(a), transportation and receipt of child pornography, are presently located at the premises and vehicle described in **ATTACHMENT A.**

GLOSSARY OF TERMS APPLICABLE TO THIS AFFIDAVIT

6. INTERNET SERVICE PROVIDER: A company that provides its customers with access to the Internet, usually over telephone lines or cable connections. Typically, the customer pays a monthly fee, and the Internet Service Provider supplies software that enables the customer to connect to the Internet by a modem or similar device attached to or installed in a computer.

7. THE INTERNET: The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across county, state, and national boundaries.

8. INTERNET PROTOCOL ADDRESS (IP Address): the unique numeric address of a machine or computer attached to and using the Internet. This address is displayed in four blocks of numbers, as in 123.456.789.001, just for example. Each numeric address can only be used by one computer or device over the Internet at a time.

9. PEER-TO-PEER FILE SHARING (P2P File Sharing): file sharing refers to the providing and receiving of digital files over a network, usually following the peer-to-peer (P2P) model, where the files are stored on and served by personal computers of the users. Most people who engage in file sharing on the Internet both provide (upload) files and receive (download) files. P2P file sharing is distinct from file trading in that downloading files from a P2P network does not require uploading, although some networks either provide incentives for uploading, such as credits, or force the sharing of files being currently downloaded.

10. TORRENT: a torrent file is a computer file that contains information about files and folders to be distributed over the BitTorrent Network. The torrent file usually contains a list of the network locations of trackers, which are computers that help participants in the system find each other and form efficient distribution groups called swarms. A torrent file does not contain the content to be distributed; it only contains information about those files, such as their names, sizes, folder structure, and hash values for verifying the integrity of the files referenced.

11. BITTORRENT NETWORK: BitTorrent is a protocol for peer-to-peer file sharing; it requires secondary support to search for files and to find peers with those files. Users start by searching for *torrent* files by using an Internet search engine to find sites that offer torrent files and by describing the content by the use of keywords they want to download. Any user may create a *torrent*; each *torrent* describes a set of files that can be obtained through the BitTorrent protocol and provides enough information to enable this process. At a minimum, this information includes file names, sizes, and Secure Hash Algorithm-1 hash values for pieces of files of a size typically between 32 KB and 16 MB each, as well as the URLs of one or more trackers, which provide a list of files available for transfer. Torrents usually also contain an extensive comment field. Along with file names described by the torrent, this comment field is typically used by web-based torrent aggregation and search sites such as isohunt.com and piratebay.org to allow users to quickly find torrents of interest by using a simple text search. The BitTorrent protocol can be used to reduce the server and network impact of distributing large files. Rather than downloading a file from a single source server, the BitTorrent protocol allows users to join a "swarm" of hosts to download and upload from each other simultaneously. The protocol is an alternative to the older single source, multiple mirror sources technique for distributing data, and can work over networks with lower bandwidth. Using the BitTorrent

protocol, several basic computers, such as home computers, can replace large servers while efficiently distributing files to many recipients. Pieces are typically downloaded non-sequentially and are rearranged into the correct order by the BitTorrent Client, which monitors which pieces it needs, and which pieces it has and can upload to other peers. Pieces are of the same size throughout a single download (for example a 10 MB file may be transmitted as ten 1 MB pieces or as forty 256 KB pieces). Due to the nature of this approach, the download of any file can be halted at any time and can be resumed at a later date without the loss of previously downloaded information, which in turn makes BitTorrent particularly useful in the transfer of larger files. This also enables the client to seek out readily available pieces and download them immediately, rather than halting the download and waiting for the next (and possibly unavailable) piece in line, which typically reduces the overall time of the download.

12. VUZE: Vuze software is an open-source free peer-to-peer BitTorrent client. Vuze is the only client that makes Clearnet (commonly known as the surface web) torrents available on I2P (Invisible Internet Project which is an anonymous network that uses end-to-end encryption) is capable of preparing, requesting, and transmitting any type of digital file over the BitTorrent network. Released under the GNU General Public License, several versions of Vuze are available and is a free software download.

13. ACCURINT: Accurint is a widely used and accepted as a tool to locate and research publicly available records. Accurint is used by government, commercial, and law enforcement agencies to obtain publicly available information and has been utilized by myself numerous times in previous investigations over twenty-three years. Accurint has proved reliable in each previous investigation.

14. SECURE HASH ALGORITHM VERSION 1 (SHA-1): the SHA hash function was designed by the National Institute of Standards and Technology (NIST) and the National Security Agency and published by the NIST as a U.S. Federal Information Processing Standard. Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States government for use by all non-military government agencies and by government contractors. The SHA-1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest (digital fingerprint), or to find two different messages which produce the same message digest as referenced in the FIPS Publication 180-1.

TECHNICAL BACKGROUND

15. Your affiant has received extensive online undercover training as well as computer forensics training in reference to computer related criminal investigations. Your affiant knows all of the below-described information as the result of his training and experience in the investigation of computer-related crime and by conferring with other law enforcement personnel who investigate computer-related crime.

16. Your affiant knows that computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It also has revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to

prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

17. The advancement in technology of computers, smartphones and tablets has added to the methods used by child pornography collectors to interact with and sexually exploit children. Each of the above serves six functions in connection with child pornography. These are production, communication, distribution, receipt, advertisement and storage.

18. Child pornographers can now produce both still and moving images directly from a common video camera, small action style cameras such as a GoPro, smartphones, laptop computers equipped with web cameras, and tablets. In the past, a camera could be attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred, or printed directly from the computer, external hard drive, media card (SD, Compact Flash, micro-SD, memory stick), smart phone, tablet, iPod or iPad. The captured image can be edited in very similar ways to a photograph. The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is inexpensive and technically easy to produce, store, and distribute child pornography. There is the added benefit to the pornographer that this method of production does not leave as large a trail for law enforcement to follow, as had been the case in the past. Your affiant has been involved in recent investigations where digital cameras, smart phones, tablets and webcams were used to produce child

pornography and store said child pornography either on the device, personal computer or removable media of the subject.

19. New technology now allows child pornographers to use even smaller digital devices like smartphones and tablets that have digital cameras and video recording capability built directly into the devices. These devices are equipped with their own processors and memory that allow the devices to actually perform as small minicomputers. With the use of free and publicly available apps, a child pornographer has the ability to produce child pornography, receive and distribute it in a matter of just a few seconds and maintain relative anonymity using free open wireless access points.

20. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. The development of the computer also has changed that. A device known as a modem allows any computer to connect to another computer through the use of telephone and/or cable lines. By connecting to a host computer, electronic contact can be made with literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. These host computers are sometimes operated by commercial concerns, such as Bellsouth, AT&T and America Online, which allow subscribers to dial a local number and connect to a network which is in turn connected to their host systems. Today many ISPs, such as Comcast Communications and Charter Communications, offer high-speed broadband Internet service. Broadband is often called high-speed Internet because it usually has a high rate of data transmission much higher than the dial-up or DSL structure of the past. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web. Some of

these systems offer their subscribers the ability to communicate publicly or privately with each other in real time in the form of "chat rooms" and/or instant messaging.

21. These communication structures are ideal for individuals who possess, receive and distribute child pornography. They provide open and anonymous communication, allowing users to locate other persons who share their interest in child pornography, while maintaining their anonymity. Once contact has been established, it is then possible to send text messages, graphic images, and high-resolution video to other individuals interested in child pornography. Moreover, the child pornographer need not use the large service providers. Child pornographers can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages are well known and are the foundation of transactions between child pornographers.

22. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. For example, child pornography can be transferred via electronic mail to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services, P2P services and easy access to the Internet, computers, tablets and smartphones are a preferred method of receipt and distribution of child pornographic materials.

23. The computer's capability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly consisting

of hard drives) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of two terabytes are not uncommon. The KPD-ICAC computer examiners routinely examine computer hard drives of 1 Terabyte (1000 gigabytes) and more in child pornography cases. These drives can store hundreds of thousands of images and video at very high resolution and quality. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, save the image, and store it at another location. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful examination of electronic storage devices is it possible to recreate the evidence trail.

24. Based on your affiant's knowledge, training and experience and training and experience of other officers, your affiant knows that child pornographers commonly download and save some of their collection of child pornography from their computer to removable media such as thumb drives, CD-ROMs, external hard drives, media cards (SD, Compact Flash, micro SD, memory stick), smart phones, smart televisions, computer game consoles (Sony PlayStation, Xbox), tablets, iPods or iPads so the images can be maintained in a manner that is both mobile and easily accessible to the collector. It is not uncommon for the child pornographer to print pictures of child pornography and to keep them in a safe and secure location for easy viewing. Thumb drives, CD-ROMs, external hard drives, media cards (SD, Compact Flash, micro-SD, memory stick), smart phones, smart televisions, computer game consoles (Sony PlayStation, Xbox), tablets, iPods or iPads, containing child pornography and printed pictures of child pornography are not only kept near the computer, but also in hidden areas known to the child pornographer, to keep other individuals from discovering the illegal material. For example, a search warrant executed by other officers known to your affiant resulted in the finding of a hard

drive wrapped in plastic hidden under a bathroom sink. Additionally, your affiant knows that in 2014, investigators with the KPD-ICAC Task Force arrested a subject for the interstate travel to meet a minor for sexual purposes (18 U.S.C. § 2423(a)). An external hard drive was located in the trunk of the suspect vehicle. A search warrant on the external hard drive revealed a contact offense by the subject on a four-year-old girl and numerous pornographic videos of the sexual abuse produced by the subject utilizing his smartphone. In a recent 2023 investigation a Dell All-in-One Desktop was located in the vehicle of the suspect and it was found to contain child pornography.

25. Your affiant states that computer technology can be mobile in the form of laptop computers, removable thumb drives, removable hard drives, media cards (SD, Compact Flash, micro-SD, memory stick), computer game consoles (Sony PlayStation, Microsoft Xbox), smart phones, iPad's, iPod's, tablets, or accessible via remote or wireless means. Therefore, evidence, contraband, instrumentalities, or fruits of crime can be located virtually anywhere within the residence or vehicle of a child pornographer. Your affiant has been involved in child pornography investigations where child pornography was found on removable media located in a suspect's vehicle. Additionally, child pornography can remain on devices indefinitely unless the user takes active steps to delete or overwrite the digital files of child pornography. Your affiant is aware of a current Knoxville Police in an investigation that originated as a P2P file sharing investigation in 2015. The computer examination of this 2015 case located child pornography files stored on the suspect computer hard drive dating back to 2009. Additionally, recent investigations have revealed that some P2P suspects in order to remain safer have instituted the methodology of downloading child pornography then deleting it after a short period of time. Based on information your affiant has gained in his interviews with child pornographers that

utilized the above-described method, the suspects indicated they felt an increased level of security knowing the child pornography was not stored on the computer/devices for long periods of time and that they could re-download mass amounts of child pornography at any time very quickly. However, computer exams have revealed that even if the above methodology is utilized examiners are able to locate and recover evidence about the criminal activity including but not limited to the files child pornography, software used to locate and download child pornography, and log files identifying specific child pornography files that have been downloaded to the computer system of the suspect.

26. A current and growing phenomenon on the Internet is P2P file sharing. P2P file sharing is a method of communication available to Internet users through the use of special software. The software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers together. While there are several P2P networks currently operating, one of the most predominant networks is the BitTorrent network. There are several different software applications that can be used to access these networks, but these applications operate in essentially the same manner. Additionally, the software applications used for P2P file sharing are generally free to download, install, and utilize.

27. Your Affiant knows from training and experience that P2P networks are frequently used in the receipt and distribution of child pornography. Your affiant knows that one network, known as the BitTorrent network, is being used to trade digital files, including still image and movie files, of child sex abuse. Based on training and experience and communication with other law enforcement offices and agents, your affiant has learned the following about the operation of the BitTorrent file-sharing network:

a) The BitTorrent network is a very popular and publicly available P2P file-sharing network. Most computers that are part of this network are referred to as "peers" or "clients." A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients.

b) The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include the BitTorrent client program, Vuze client program, uTorrent client program, and BitComet client program, among others. These client programs are publicly available and typically free P2P client software programs that can be downloaded from the Internet.

c) During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files via automatic uploading. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other users (peers/clients) on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files, a process referred to as "seeding."

d) Files or sets of files are shared on the BitTorrent network via the use of "Torrents." A "Torrent" is typically a small file that describes the file(s) to be shared. It is important to note that "Torrent" files do not contain the actual file(s) to be shared. Rather the "Torrent" contains only the information about the file(s) to be shared and information needed to accomplish a download of the file(s) to be shared. This information includes things such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent." The

"info hash" is a SHA-1 hash value of the set of data describing the file(s) referenced in the "Torrent." This set of data includes the SHA-1 hash value of each file piece in the torrent, the file size(s), and the file name(s). The "info hash" of each "Torrent" uniquely identifies the "Torrent" file on the BitTorrent network. The "Torrent" file may also contain information on how to locate file(s) referenced in the "Torrent" by identifying "Trackers." "Trackers" are computers on the BitTorrent network that collate or index information about the peers/clients that have recently reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the network who may be sharing part or all of the file(s) referenced in the "Torrent." "Trackers" do not actually have the file(s) but are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of "Tracker(s)" on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular "Torrent" file. There are many publicly available servers on the Internet that provide BitTorrent tracker services.

e) In order to locate "Torrent" files of interest and download the files that they describe, a typical user will use keyword searches on torrent indexing websites, examples of which include isohhunt.com and the piratebay.org. Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate "Torrent" files that describe the files they are looking to download. Torrent indexing websites do not actually host the content (files) described by "Torrent" files, only the "Torrent" files themselves. Once a "Torrent" file is located on the website that meets a user's keyword search criteria, the user will download the "Torrent" file to their computer. The BitTorrent network client program on the user's computer will then process that "Torrent" file in order to find "Trackers" or utilize other

means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent" file. It is again important to note that the actual file(s) referenced in the "Torrent" are actually obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA-1 "info hash" value comparison), or parts of the same file(s), referenced in the "Torrent," to include the remote peers/clients IP addresses.

f) For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a torrent indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). The results of the keyword search are typically returned to the user's computer by displaying them on the torrent indexing website. Based on the results of the keyword search, the user would then select a "Torrent" of interest to them to download to their computer from the website. Typically, the BitTorrent client program will then process the "Torrent" file. Utilizing trackers and other BitTorrent network protocols, peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the "Torrent" file available for sharing. The file or files are then downloaded directly from the computer(s) sharing the file or files. Typically, once the BitTorrent network client has downloaded part of a file or files, it may immediately begin sharing the part of the file or files it has with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA-1 hash value of that piece which is described in the "Torrent" file. The downloaded file or files are then stored in an area (folder) previously designated by the user and/or the client program on the user's computer or designated external storage media. The

downloaded file or files, including the torrent file, will remain in that location until moved or deleted by the user.

g) Law Enforcement can search the BitTorrent network in order to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. Searching the BitTorrent network for these known torrents, Law Enforcement can quickly identify targets in their jurisdiction. Law Enforcement receives this information from "Trackers" about peers/clients on the BitTorrent network recently publicly reporting that they are involved in sharing digital files of known or suspected child pornography, based on "info hash" SHA-1 hash values of torrents. These torrents being searched for are those that have been previously identified by law enforcement as being associated with child pornography files. There are BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file or files are downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

h) During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator's BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes:

1. The suspect client's IP address;

2. A confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) are being reported as shared from the suspect client program; and

3. The BitTorrent network client program and version being utilized by the suspect computer. Law enforcement has the ability to log this information.

i) This investigation of P2P file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the ICAC Task Force Program. Many of the officers involved in this effort are using the technology and methods described herein. This methodology has led to the issuance and execution of search warrants around the country resulting in many seizures of child pornography; arrests for possession, receipt and distribution of child pornography; and the identification of victims of child sexual abuse. Your affiant has been investigating P2P file sharing networks since 2007.

28. The computers that are linked together to form the P2P network are located throughout the United States and throughout the world; therefore, the P2P network operates in interstate and foreign commerce. A person that includes child pornography in his/her "shared" folder is hosting child pornography and therefore is promoting, presenting, and potentially distributing child pornography. A person that hosts child pornography is in violation of Title 18, United States Code, Section 2252A(a)(3)(B), in that he/she is promoting and presenting child pornography in interstate and foreign commerce by means of a computer.

29. Even though the P2P network links together computers all over the world and users can download files, it is not possible for one user to directly send or upload a file to another user on the P2P network. The P2P software is designed only to allow files that have been

selected by the user to be downloaded. Using the P2P software, one does not have the ability to send files from his/her computer to another user's computer without their permission or knowledge. Therefore, it is not possible for one user, using the P2P software; to send or upload child pornography files to another user's computer without his/her active participation.

THE INVESTIGATION

30. This affidavit is submitted in support of the issuance of a warrant authorizing the search of the premises described in ATTACHMENT A, along with the digital media found there, in order to locate and seize the items described in ATTACHMENT B.

31. An authorized undercover investigation has revealed that a computer accessing the BitTorrent Network using the IP address of 73.113.119.223 has been observed on the BitTorrent network, possessing and offering to participate in the distribution of child pornography between the dates of March 11, 2023, and April 21, 2023.

32. On March 11, 2023, while connected to the Internet in an authorized online undercover capacity, your affiant launched a BitTorrent application to locate computers, possessing, advertising and distributing images and or videos of child sex abuse within the Eastern District of Tennessee.

33. Between March 12, 2023, and March 13, 2023, your affiant identified a computer/device within the state of Tennessee with the IP address of 73.113.119.223 as advertising and potentially distributing files containing child pornography. Your affiant directed the investigative focus to the computer/device at IP address 73.113.119.223 because it was associated with a torrent file with the following infohash: cbcbe160116a5afdbd91bef955199794a3d9be2d.

34. In this particular case the torrent file identified by the infohash: cbcbe160116a5afdbd91bef955199794a3d9be2d, references 10,087 files. Your affiant was able to download multiple image and video files which depict child pornography referenced in the above torrent file with infohash: cbcbe160116a5afdbd91bef955199794a3d9be2d. Your affiant knows that numerous files downloaded from the device using 73.113.119.223 were child pornography by personally reviewing the files downloaded. Your affiant has seen these downloaded files in previous child pornography cases. The child pornography files were directly downloaded from the single source IP address of 73.113.119.223.

35. On March 12, 2023, at 17:51:44 (GMT-04:00), your affiant successfully completed the download of two of the files referenced by the torrent that the Suspect Device was advertising and making available for distribution. Below is a description of those files. The files were in the suspect's shared folder at the time of the undercover connection.

(1) File "001432.mpg" – "5yo daughter Edyta – Unloading on her ass while she's asleep.mpg". The file has a SHA-1 hash value of DE57285E9CD3ACA72DFB080C9C62972378410291. The file is a color video and is approximately 1:00 minutes in length. The file depicts a minor female approximately 5 years old lying on a bed apparently sleeping. She has on a pink shirt and no underwear. She is lying on her right side with her left leg pulled up toward her chest. It appears that there is a laptop computer in the background playing a pornography video. An adult male is seen kneeling over the child's buttocks while he masturbates. The adult male ejaculates on the minor child's buttocks.

(2) File "001466" – "MOV00300.avi". The file has a SHA-1 hash value of

75f61e1d0bbfc6ec597fab43c8c0b720e6a2057b. The file is a color video file with sound and is 7 minutes and 31 seconds in length. The file depicts a young minor girl approximately 4 years old on a bed with no underwear and wearing a pink and red striped long sleeve shirt. The child is shown watching television while an adult male spreads her legs and videotapes her vagina. The child attempts to cover herself with a blanket but the adult male pulls it away and continues to videotape the child. The adult male is seen spreading the vagina of the child and rubbing her vagina with his fingers.

36. Your affiant has downloaded approximately 900 additional files comprised of child pornography images and child pornography videos between the dates of March 11, 2023, and April 21, 2023, from the suspect device at IP address 73.113.119.223. The images and videos depict children under the age of eighteen (18) years old engaged in sexually explicit conduct and/or poses and is believed to be child pornography in violation of Title 18, United States Code, Section 2252A(a)(2), which make it a crime for any person to distribute child pornography in interstate or foreign commerce, by any means, including by computer.

37. On March 12, 2023, a domain name system (DNS) check on the IP address 73.113.119.223 was conducted through the American Registry for Internet Numbers (ARIN). Your affiant received information that the IP address 73.113.119.223 was registered to Comcast Communications, LLC. Investigators have used ARIN since 2000 as an investigative resource and it has proved to be reliable in every case.

38. On March 20, 2023, A State of Tennessee Administrative Subpoena was issued by the District Attorney General's Office 7th Judicial District to Comcast Communications, LLC for the production of records associated with the IP address of 73.113.119.223 for the date of March 12, 2023, at 09:45 PM UTC.

39. On or about April 04, 2023, Comcast Communications, LLC responded to the request for the production of records pertaining to the IP address of 73.113.119.223, and provided the following information:

Subscriber Name:	MICHAEL POTTER
Service Address:	118 MASON AVE LAKE CITY, TN 3776-92710
Billing Address:	118 MASON AVE LAKE CITY, TN 3776
Telephone #:	(248) 921-1172
Type of Service:	INTERNET (No additional services)
Account Number:	8396500190043061
Start of Service:	Unknown
Account Status:	Active
IP Assignment:	Dynamically Assigned
IP History:	73.113.119.223 (note: during time of downloads)
E-mail User Ids:	gamedragonexe@comcast.net

40. Your affiant conducted a law enforcement database check of the TN Criminal Justice Portal. It showed Michael Robert Potter with a date of birth of 01/26/1987 and a TN OLN #127687684, at the address of 9118 Mason Ave. Rocky Top. TN 37769. Note: In 2014 Lake City, TN was renamed to Rocky Top, TN.

41. On May 29, 2020, your affiant conducted a search on ACCURINT of publicly available information for residents at 118 Mason Ave. Rocky Top, TN 37769. Your affiant received information that Michael Robert Potter, with a date of birth of 01/26/1987 was residing

at 118 Mason Ave. Rocky Top, TN 37769 as well as a Karli Kay Tumbleson with a date of birth 06/08/1992.

42. On June 28, 2023, Anderson County Sheriff's Detective Luethge conducted surveillance of 118 Mason Ave. Rocky Top, TN 37769. The residence was observed as a one-story structure with light beige vinyl siding and green shutters and green roof. The residence has a front porch with a wooden latticed railing and steps leading up the porch to a green front door. A short gravel driveway is to the left of the structure with a silver mailbox in front of the residence with the numbers "118" in black on the box and a green placard attached to the mailbox post with the numbers "118" on it.

43. Additionally, Detective Luethge observed a Black Chevrolet SUV with TN tag # BPS-5815 currently registered to Michael Potter at 118 Mason Ave. Rocky Top, TN 37769. Detective Luethge also observed a blue Ford Fusion with TN Tag# BGQ-1921 registered to Karli Tumbleson at 118 Mason Ave. Rocky Top, TN 37769.

44. There were several wireless Wi-Fi signals detected that were all secure and require a password or passcode to connect.

CONCLUSION

45. Based on the aforementioned information, your affiant respectfully submits that there is probable cause to believe that a computer and/or electronic devices located at 118 Mason Ave. Rocky Top, TN 37769, are advertising, possessing, receiving and distributing child pornography. Your affiant bases this belief on the fact that on March 11, 2023, and April 21, 2023, a computer utilizing the file sharing software known as Vuze software (version: - AZ5760-) and using the IP address of 73.113.119.223 possessed, received, advertised, and distributed files of child pornography and that said files of child pornography were located in a "shared" folder of

the subject computer advertised and distributed over the Internet to the KPD-ICAC Task Force undercover computer.

46. Based on the investigation, uploads of child pornography to the internet have occurred by a user using the Comcast internet at 118 Mason Ave, Rocky Top, TN 37769. The Knoxville Police Department's ICAC Task Force, currently conducts onsite previews of computers in order to focus and seize only devices containing contraband. This process assists investigators with only seizing and examining items associated with the criminal activity. Based on experience, cooperation from occupants of the residence being searched assists investigators with identifying and seizing only devices that will contain contraband. It is important to note that systems currently powered off will not be powered on to conduct a preview unless investigators believe turning on the device will not alter or destroy possible evidence.

47. Your affiant knows from experience that anyone in the residence can access the internet once a subscription to internet services is created. Your affiant knows from experience that most often individuals participating in the sexual exploitation of children by the collecting and trading of child pornography almost exclusively create fictitious accounts to indulge in criminal activity as well as utilize anonymous Peer to Peer file sharing networks. Although the IP address is an excellent source of information where the physical criminal activity has occurred, it cannot pinpoint which person within the household is the criminal suspect. Your affiant knows from personal experience that the offender literally could be anyone in the household to include one or both parents, sons and daughters (both minors and adult children). Your affiant knows from experience that devices in the home are sometimes shared between users, that old devices such as smart phones and laptops although no longer used can still access WIFI internet signals and be used by the offender to traffic in child pornography. Your affiant

knows from experience that to successfully identify the offending device or devices that all of the devices in the residence may need to be examined or previewed onsite. Your affiant does not want to seize every piece of electronic equipment in the household or in the vehicle listed, however, it is critical that the process described in paragraph 46 be used to locate the offending device or devices. It has been your affiant's experience, that the on-scene screening process is less intrusive and less burdensome to the innocent individuals in the household who can quickly have their electronic devices returned to them.

48. Based on experience and knowledge of these cases, your affiant believes there is probable cause to believe that the electronic devices which are most likely portable (such as laptop computers and cell phones) could possibly be stored in the following vehicle: a Black Chevrolet SUV TN Tag #BPS-5815 registered Michael Potter located at 118 Mason Ave, Rocky Top, TN 37769. Your affiant has investigated cases where the subject had stored images of the sexual abuse of his girlfriend's minor daughter on an external hard drive and transported that hard drive in the trunk of his car to Knoxville, Tennessee. Additionally, your affiant executed a search warrant in August 2023 where an all-in-one desktop computer was located in the subject's vehicle. Upon examination it was determined that the all-in-one contained a significant amount of child pornography.

49. Based on the foregoing, there is probable cause to believe that a computer and/or electronic device located at 118 Mason Ave. Rocky Top, TN 37769, has been used in conjunction with violations of Title 18, United States Code, Section 2252A(a)(1), which makes it a crime for any person to ship or transport child pornography in interstate or foreign commerce; Title 18, United States Code, Section 2252A(a)(2), which makes it a crime to knowingly receive or distribute child pornography that has traveled in interstate and foreign commerce; and Title

18, United States Code, Section 2252A(a)(5), which makes it a crime for any person to knowingly possess or access with intent to view material that contains an image of child pornography, as defined in Title 18, United States Code, Section 2256(8).

50. Further, there is probable cause to believe that evidence, fruits and instrumentalities of this crime, which are listed specifically in Attachment B, which is incorporated herein by reference, are presently located on the premises described in Attachment A. Rule 41 of the Federal Rules of Criminal Procedure authorizes the government to seize and retain evidence and instrumentalities of a crime for a reasonable time and to examine, analyze and test them.

51. The evidence, fruits and instrumentalities of violation of Title 18, United States Code, Section 2252, believed to be concealed at the premises described in Attachment A, are listed in Attachment B of this affidavit, which is incorporated herein.

52. Therefore, your affiant respectfully requests issuance of a search warrant authorizing the search and seizure of the items listed in Attachment B.

53. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

Thomas Evans

Thomas Evans- Task Force officer with HSI
Investigator
Knoxville Police Department
Internet Crimes Against Children Task Force

Sworn and subscribed before me this 22nd day of September, 2023.

Jill E McCook

JILL E. McCOOK
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF PREMISES AND VEHICLE TO BE SEARCHED

Premises:

The residence is located at 118 Mason Ave. Rocky Top, TN 37769 in the Eastern District of Tennessee. The residence is a one-story house with beige siding and a green roof. Shutters on the windows are green in color as well as the front door. The residence has a front porch with wooden lattice. The mailbox is silver in color with the numbers "118" on the side. A green placard is in front of the house near the driveway. The mailbox post has the numbers 118 on the green placard.

Physical Description of Premises:

Construction Type: The residence in a one-story house with beige siding and a green roof. Shutters on the windows are green in color as well as the front door. The residence has a front porch with wooden lattice. A tile of light-colored mortar located on the front of the house shows the address of 118 Mason Ave, Rocky Top, TN 37769.

Vehicle:

Black Chevrolet SUV TN tag BPS-5815 registered to Michael Potter at 118 Mason Ave, Rocky Top, TN 37769 located at the above stated premises at time of the execution of the search warrant.

ATTACHMENT B

Below is a list of items to be searched and seized from the premises and vehicle described in ATTACHMENT A:

1. Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), monitors and or televisions, flatbed scanners and data where instrumentalities of and will contain evidence related to this crime. The following definitions apply to the terms as set out in this affidavit:

(a) Computer Hardware:

Computer hardware consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to central processing units; internal and peripheral storage devices such as thumb drives, CD-ROMs, external hard drives, media cards (SD, Compact Flash, micro SD, memory stick), smart phones, computer game consoles (Sony PlayStation, Xbox), tablets, iPods or iPads, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printers, video display monitors, and related communication devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

(b) Computer Software:

Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

(c) Documentation:

Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.

(d) Passwords and Data Security Devices:

Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

2. Any and all notes, documents, records, or correspondence pertaining to child pornography as defined under Title 18, United States Code, Section 2256 (8).

3. Any and all correspondence identifying persons transmitting, through interstate commerce including the United States mail or computers, any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

4. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

5. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

6. Child pornography in any form.